Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

INTRODUCTION TO SUBSTITUTION GROUPS.

By G. A. MILLER, Ph. D., Leipzig, Germany.

[Continued from March Number.]

Having disposed of the regular primitive groups we turn now to those whose order exceeds their degree. We have proved that all of these involve n conjugate subgroups whose degree is at most equal to $n-1$. Suppose the degree of these subgroups were $n-2$. Without loss of generality we may then assume that the following identities are satisfied :

$$G_1 \equiv G_2,\ G_3 \equiv G_4,\ \ldots\ldots\ G_{n-1} \equiv G_n.$$

If g_1 represents the order of G_1 we see that $2g_1$ substitutions of G transform G_1 into itself, viz., those which replace a_1 by itself and those which replace a_1 by a_2. All of the g_1 substitutions which replace a_1 by a_2 must therefore also replace a_2 by a_1, *i. e.*, contain the cycle a_1a_2. Similar remarks apply to the other couples a_3a_4, $\ldots\ldots a_{n-1}a_n$.

We inquire whether these couples may be used as systems of non-primitivity. We have already proved that every substitution that replaces one letter of a couple by the other contains the couple as a distinct cycle. It remains to show that the couples are interchanged as units by the substitutions of G. Suppose one of these substitutions t replaces a_1 by a_3. Then will

$$t\,G_3t^{-1} = G_1$$

t must therefore replace a_2 by a_4. Since similar remarks apply to the other couples we have proved that the couples can be used as systems of non-primitivity.

In an exactly similar way we can prove the general case that if the degree of the conjugate subgroups is $n-\alpha$ $(\alpha > 1)$ then systems of α letters each may be used as systems of non-primitivity. Hence the

THEOREM. *Whenever a transitive group contains a subgroup whose degree is less than* $n-1$ *and which involves all the substitutions that do not contain a given letter it must be non-primitive.*

Having developed some of the most important properties of the subgroups of G which do not contain a given letter we proceed to inquire into their substitutions. Suppose that among the substitutions of a transitive group G

$$a_1\,a_\alpha$$

has only one solution ; *i. e.*, there is only one cycle of this type in the group which contains a_1. Then there can be only one value of γ for each β in

$$a_\beta \, a_\gamma \qquad (\beta=1,\ 2,\ \ldots\ldots n)$$

since any a can be transformed into a_1. All the conjugates of $a_1 a_\alpha$ are therefore distinct and may be used as systems of non-primitivity of the given transitive group.

More generally speaking we may say that if G contains a subgroup G' whose degree n' is less than the degree of G and if any given letter of G (a_1) is found in only one of the transforms of G' with respect to G, then will these transforms

$$G',\ G'',\ \ldots\ldots,\ G^n$$

constitute systems of non-primitivity of G.

For if G^α and G^β had a common letter then would the substitution of G which transforms this common letter into a_1 lead to two such groups both of which would involve a_1. This is contrary to the hypothesis. These conjugate subgroups must therefore involve distinct sets of letters which may be regarded the systems of non-primitivity of G. Hence the

THEOREM. *If a primitive group contains a subgroup whose degree is less than the degree of the group it must also contain a substitution which transforms this subgroup into one which contains any one of its letters together with at least one new letter.*

From this theorem it follows that if a primitive group whose degree exceeds 2 contains the cycle $a_1 a_2$ it must also contain $a_1 a_3$ (a_3 representing any suitable letter, different from a_1 and a_2) and therefore the symmetric group of these three letters $(a_1 a_2 a_3)$all.

If a primitive group whose degree exceeds three contains $(a_1 a_2 a_3)$all it must, according to the given theorem, also contain $(a_1 a_\alpha\, a_\beta)$all where at least one of the two subscripts α, β exceeds 3. Representing this by 4 we can easily show that the group must contain at least all the substitutions of

$$(a_1 a_2 a_3 a_4)\text{all}$$

whose degree does not exceed 3. For if any such substitution is given we can find some substitution of $(a_1 a_2 a_3)$all which is either the same or differs from it only in having another letter a_α where the given substitution has a_4. The transform of this substitution with respect to $a_\alpha\, a_4$ (which is known to be in the group) will be the given substitution. Since every substitution of the fourth degree is the product of two substitutions of a lower degree the given primitive group must contain

$$(a_1 a_2 a_3 a_4)\text{all}.$$

In general, if a primitive group whose degree exceeds m contains

$$(a_1 a_2 \ldots\ldots a_m)\text{all}$$

it must also contain

$$(a_1 a_\alpha \ldots\ldots a_\mu)\text{all}$$

where the number of subscripts $1, \alpha, \ldots\ldots \mu$ is m and at least one of them exceeds m. Representing this by $m'+1$ we see that G must contain

$$a_\alpha \, a_{m+1} \qquad (\alpha = 1, 2, \ldots\ldots a_m).$$

We consider now any substitution of

$$(a_1 a_2 \ldots\ldots a_{m+1})\text{all}$$

whose degree does not exceed m. We can find some substitutions in

$$(a_1 a_2 \ldots\ldots a_m)\text{all}$$

which is either the same or differs from it only in having a_α where this has a_{m+1}. In this case the transform with respect to $a_\alpha \, a_{m+1}$ will be the given substitution. Since a substitution of the $m+1^{\mathrm{s}}$ degree ($m \eqslantgtr 2$) may be regarded as the product of two substitutions of a lower degree the given primitive group must contain

$$(a_1 a_2 \ldots\ldots a_{m+1})\text{all}.$$

Calling $m+1$ m' we can prove in the same way that G contains the symmetric group of $m'+1 = m+2$ letters, etc. Hence the

THEOREM. *Whenever a primitive group contains a symmetric subgroup of a lower degree it must be a symmetric group.*

COROLLARY. *If a primitive group contains a substitution of the form $a_1 a_2$ it is symmetric.*

We will now suppose that the primitive group contains

$$a_1 a_2 a_3.$$

If its degree exceeds 3 it must also contain

$$a_1 a_\alpha \, a_\beta$$

where at least one of the two letters, say α, is greater than 3. We shall represent this by 4, G then contains the two substitutions

$$a_1 a_2 a_3 \text{ and } a_1 a_4 a_\beta$$

and therefore

$$(a_1 a_2 a_3 a_4)\text{pos}.$$

In general, if a primitive group whose degree exceeds m contains

$$(a_1 a_2 \ldots\ldots a_m)\text{pos}$$

it must also contain

$$(a_1 a_\alpha \ldots\ldots a_\mu)\text{pos}$$

where the number of subscripts 1, α, ...μ is m and at least one of them exceeds m. Representing this by $m+1$ we see that G contains

$$a_\alpha\, a_{m+1} a_\beta \qquad (\alpha=1,\ 2,\ \ldots\ldots\ m).$$

It must therefore contain at least all of the substitutions of

$$(a_1 a_2 \ldots\ldots a_{m+1})\text{pos}$$

whose degree does not exceed m. For if s is any such substitution containing a_{m+1} there is some substitution s_1 in

$$(a_1 a_2 \ldots\ldots a_m)\text{pos}$$

which differs from s only in having a_δ where s has a_{m+1}. If β exceeds m we make $\alpha=\delta$ then will $a_\alpha\, a_{m+1} a_\beta$ transform s_1 into s. If $\beta \leqq m$ we transform the substitution

$$a_\alpha\, a_{m+1} a_\beta$$

with respect to some substitution of $(a_1 a_2 \ldots\ldots a_m)$pos. So that in place of a_β we may have a letter not found in s. Let this transform be

$$a_\gamma\, a_{m+1} a_\varepsilon \qquad (\gamma,\ \varepsilon \leqq m).$$

We now take from the substitutions of $(a_1 a_2 \ldots\ldots a_m)$pos the one s_2 which differs from s only in having a_γ where s has a_{m+1} if s does not contain a_γ, and the one s_3 which differs from s only in having a_ε, a_γ where s has a_γ, a_{m+1} if s contains a_γ. The transform of these with respect to

$$a_\gamma\, a_{m+1} a_\varepsilon$$

will be the required substitution s.

This proves that G contains all the substitutions of $(a_1 a_2 \ldots\ldots a_{m+1})$pos whose degree is equal to or less than m. These generate $(a_1 a_2 \ldots\ldots a_{m+1})$pos, for any positive substitution of the $(m+1)^{th}$ degree $(m>2)$ may be considered as the product of two positive substitutions of a lower degree. [Let $s=\ldots a_x a_y \ldots$ be any positive substitution of the $(m+1)^{th}$ degree and $s_1 \ldots\ldots a_x a_y \ldots\ldots$ be any positive substitution of a lower than the $(m+1)^{th}$ degree. Then will s_2 in

$$s=s_1 s_2 \text{ or } s_2=s_1{}^{-1} s$$

be also a positive substitution whose degree $\leqq m$].* Hence the

THEOREM. *If a primitive group contains a substitution of the form* $a_1 a_2 a_3$ *but none of the form* $a_1 a_2$ *it is the alternating group.*

We are now in possession of the following important facts in regard to any primitive group G.

(1) If $g=n$, G must be generated by a single cycle which involves a prime number of letters, and for each prime number there is one and only one such primitive group.

(2) If g does not equal n it must be a larger multiple of n and G must contain n conjugate subgroups whose degree is $n-1$ and whose order is $g \div n$.

(3) If G contains a substitution of the form $a_1 a_2$ or one of the form $a_1 a_2 a_3$ it must contain the alternating group.

(4) Both the alternating and the symmetric groups have a 1, 1 correspondence to the positive integers beginning with 2.

(5) The order of the symmetric group is $n\,!$ and that of the alternating group is $\frac{1}{2}n\,!$.

(6) The average number of letters in all the substitutions of a transitive group is $n-1$.

(7) Every transitive group contains at least $n-1$ substitutions of the n^{th} degree.

The three classes of primitive groups, regular, alternating, and symmetric, each of which contains an infinite number of members, are distinct when $n>3$. The groups that belong to these classes for any value of n are well known. It remains to determine those whose order satisfies the inequality

$$n>g>\tfrac{1}{2}n\,!.$$

Before pursuing the general discussion any farther we shall seek all the primitive groups whose degree does not exceed six. In doing this we shall use some methods which will be of service in the further study of this subject. Most of the methods, however, may serve as illustrations of the theorems which have been developed.

[To be Continued.]

---

*It can be easily proved that if a group contains

$$a_1 a_2 a_\alpha \qquad (\alpha=1,\ 2,\ \ldots\ldots n)$$

it contains the alternating group of degree n, and if it contains

$$a_1 a_\alpha \qquad (\alpha=1,\ 2,\ \ldots\ldots n)$$

it contains the symmetric group of degree n. Cole's Netto, §§ 34, 35.